UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

UMG RECORDINGS, INC., *et al*., *Plaintiffs*, v. KURBANOV, *et al*., *Defendants*.	Case No. 1:18-cv-00957-CMH-TCB

DECLARATION OF ROBERT W. SCHUMANN

1. I, Robert W. Schumann, hereby declare pursuant to 28 U.S.C. § 1746 that the statements below are true and correct to the best of my personal knowledge and belief.

2. I have knowledge of the facts set forth herein based on my personal knowledge or documents and information reviewed in connection with this case and, if necessary, I would and could competently testify thereto if called as a witness in this matter.

3. I have worked in the computer and technology industry for the past 36 years. In 1985, I received a Bachelor of Science in Computer Science from Rochester Institute of Technology. Since that time I have worked in various facets of the computer industry, in connection with the design and development of computer software, computer networking systems, computer automation, consumer electronics, large-scale database processing, drone accessories, physical and electronic Audio/Video distribution systems, digital security, and other content-protection systems. I also have been personally involved in and overseen the development and licensing of sophisticated technical specifications including: work on industry-standard specifications for digital content processing and security; and the design and development of

consumer electronics products and devices including hardware DVD players, web-based content delivery services, and the integration and licensing of third-party software packages, technologies, and associated technical specifications.

4. I have seventeen issued and pending United States Patents, many of which involve digital content protection and consumer products. I was a founding member of the Digital Watermarking Alliance, an industry trade group for digital watermarking, and I have spoken extensively at trade shows and other professional venues on content security. I have previously testified in three cases regarding web-based content delivery, circumvention, and related technology. I also testified in an arbitration as an expert on the online video industry on behalf of NBC Universal and Hulu.

5. This declaration is based upon my professional experience with computer software, computer networking systems, and various content protection technologies, as well as my usage and testing of the websites at issue.

Defendant's Websites

6. In this declaration, I refer to the websites located at the web addresses www.flvto.biz and www.2conv.com collectively as "Defendant's Websites."

7. Defendant's Websites provide users with the ability to download the audio portions of YouTube videos as audio files. YouTube does not provide this download feature. YouTube is a streaming service—the music videos on the site can be listened to and viewed by users while they are connected to the internet, but the transmission of those videos does not result in a permanent copy of the music video or just the audio portion of the music video being made for offline access by the user.

8. Each video on YouTube has a unique watch-page URL, which is the address of the video's page on the YouTube site. To use one of the Defendant's Websites, a user (1) pastes the "watch-page" URL of a desired video into a blank text box on the home page, (2) checks a box to indicate agreement to the terms of use, and then (3) clicks on a "convert" button. The final step above takes the user to new page that, after a matter of seconds, presents a link to download from Defendant's Websites an MP3 file of the audio portion of the desired video. When the user clicks on the download link, the MP3 file downloads from the Defendant's Websites' server to the user's computer.

Client-Server Model

9. Websites, including the Defendants' Websites, use what is known as the client-server model. In the client-server model, the client makes requests to the server, and the server sends responses. The user's computer (or other sort of internet-access device such as a smartphone or tablet) is the client. Specifically, the client is web browser software such as Google Chrome, Apple Safari, or Microsoft Edge running on the user's computer. Defendants' Websites operate on powerful computers in an internet data center; these computers are the servers. They are known as web servers because they are designed to respond to requests from web browsers. The most widely used web server programs include Apache, Nginx, and Microsoft IIS. These programs are standard parts of the server side of the internet.

10. When the user visits the home page of Defendant's Websites, this visit consists of a request made by the user's web browser (the client) to Defendant's Websites' web server over the internet. Each request is in effect a message that includes the external Internet Protocol ("IP") address of the user's computer (which can be used to identify the geographic location of the user)

and the URL of the resource, such as a webpage or file, that the user wishes to retrieve. The server processes the request and sends a response with the appropriate resource to the browser.

11. A web server receives each request via a network connection and necessarily maintains the request in temporary memory known as RAM (Random Access Memory) during the processing of the request. RAM is distinct from permanent storage, such as that on a hard drive, in that the contents of RAM are lost if the server is turned off.

Server Data Is Commonly Preserved

12. Site operators commonly configure their web servers to maintain logs of server activity for a variety of reasons, including the detection of errors, detection of abuse, the analysis of which site features are most popular with users, and auditing of traffic volumes for determining advertising revenue. Web servers maintain these logs on permanent storage media such as hard drives that are attached or otherwise local to the web servers. These media are permanent in the sense that they retain their data even when powered off. Servers may be configured to store logs indefinitely or for a certain period such as 30 days, after which they are deleted from the storage medium.

13. The popular web server programs mentioned above, and other comparable ones, include functionality for logging each request and the fact and nature of the response to each request (but not the full response itself). The request log, commonly referred to as an access log, includes the time and date, IP address, and URL of each request.

14. Site operators may supplement local logging with remote logging to remote third-party services such as Google Analytics and Yandex Metrica that provide sophisticated reporting functionality. These are also referred to as web analytics services. A site operator using a remote logging service defines, via the program code of their website, precisely which events should be

remotely logged. The site operator's web server will typically effect this remote logging functionality by including instructions within the responses to the client browser, and the client browser than actually makes the calls to the remote logging service.

Defendants' Server Data

15. In general, it is impossible for an outsider in the position of a site user, with no administrative access to the site's web server, to determine whether a site is engaging in local logging. The nature of the remote logging services, however, is that their use is easily apparent, even to an outsider, because each logged event results in a distinct and visible interaction between the user's browser and the remote logging service.

16. As described above, ordinary use of Defendant's Websites involves the click of a "convert" button and the subsequent click of a link to download the MP3 audio file that has been "ripped" from a YouTube music video. Each of these "convert" and "MP3 download" events generates distinct requests from a user's browser to the Defendant's Websites that are of the sort that would be locally recorded by web server software with logging activated.

17. The "convert" request generated by a click of the "convert" button contains the watch-page URL of the video for which the user desires the audio portion. The "MP3 download" request contains the filename of the ripped MP3 file, which, in the case of music, often contains the name of the artist and the title of the song. The corresponding log entries for these events on Defendants' Websites (if the server data is preserved) would identify the event date/time and geographic region of the user. Among other things, the log entries as whole would indicate the volume of usage of Defendant's Websites.

18. According to observable responses generated by the Defendant's Websites, the web server program in use by Defendant appears to be Nginx—though that information is preliminary,

not definitive, and not a substitute for technical discovery from Defendant. In addition, Defendant's Websites use the Yandex Metrica remote logging service to record each "convert" request and each "MP3 file download" request.

19. This declaration is meant to assist the Court's consideration of Plaintiffs' motion to compel. It is not meant as a wholesale examination of all the technological aspects of Defendant's Websites that may be relevant in this case.

Executed on June 16th, 2021

Robert W. Schumann